



US005506905A

United States Patent [19]

Markowski et al.

[11] **Patent Number:** 5,506,905[45] **Date of Patent:** Apr. 9, 1996[54] **AUTHENTICATION METHOD FOR
KEYLESS ENTRY SYSTEM**[75] Inventors: Dale W. Markowski, West Milwaukee,
Wis.; Oddy N. Khamharn, Gurnee,
Ill.; Mark E. Bianco, Pomona, Calif.

[73] Assignee: Delco Electronics Corp., Kokomo, Ind.

[21] Appl. No.: 257,982

[22] Filed: Jun. 10, 1994

[51] Int. Cl.⁶ H04L 9/32

[52] U.S. Cl. 380/25; 380/23

[58] Field of Search 380/23-25, 49,
380/50[56] **References Cited****U.S. PATENT DOCUMENTS**

5,103,221	4/1992	Memmola	340/825.34
5,191,610	3/1993	Hill et al.	380/25
5,369,706	11/1994	Lake	380/23
5,398,284	3/1995	Koopman, Jr. et al.	380/49
5,420,925	5/1995	Michaels	380/23

OTHER PUBLICATIONSClifford advertisement, Car Audio & Electronics, May 1994,
vol. 7, p. 75.

Viper advertisement, Car Audio & Electronics magazine,

May 1994, vol. 7, p. 73.

"Code Grabbing," Car Audio and Electronics magazine,
May 1994, vol. 7 pp. 72, 74, 76.*Primary Examiner*—Salvatore Cangialosi
Attorney, Agent, or Firm—Mark A. Navarre

[57]

ABSTRACT

A system for remotely controlling a desired door locking or other function in a vehicle or other protected environment has a transmitter and receiver for communicating a message including a sequence number, the code of a selected function to be performed and an authenticator. An algorithm in the transmitter and in the receiver has a cryptographic key and a seed code. Each algorithm generates the authenticator as a function of both the seed code and the function code; if the authenticators are equal, the message is valid. Upon each transmission the seed code is updated and the sequence number is incremented. The receiver updates its seed code according to the transmitted sequence number to keep the algorithms in synchronism.

13 Claims, 2 Drawing Sheets

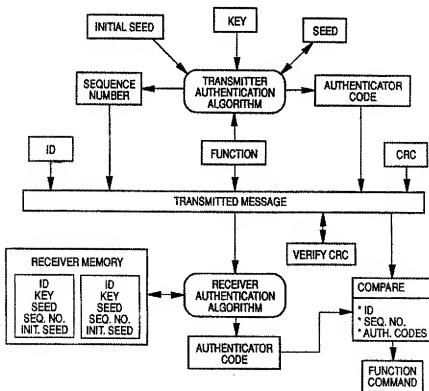
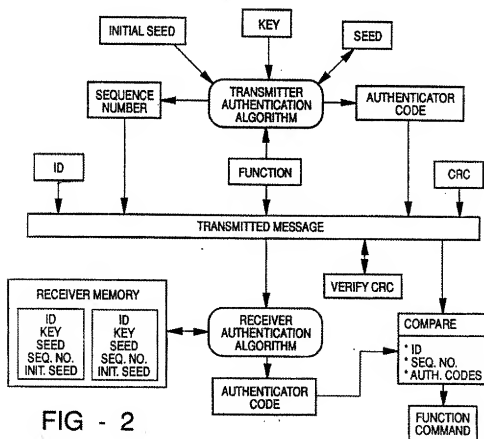
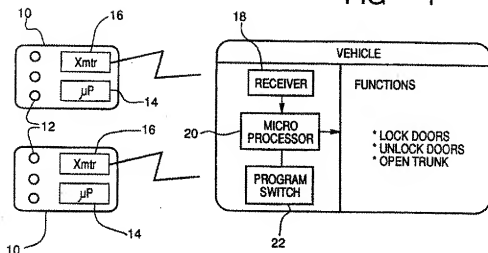


FIG - 1



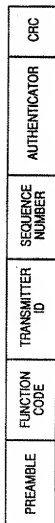
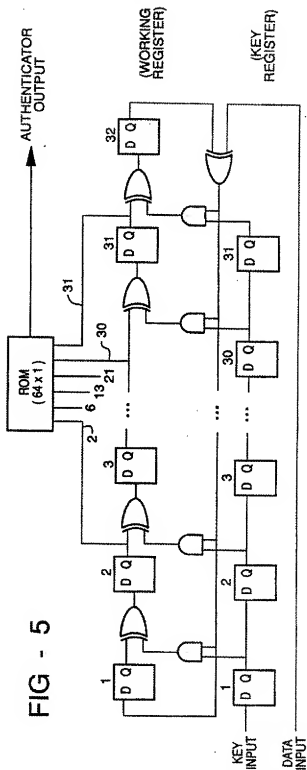
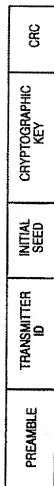


FIG - 4

FIG - 3



AUTHENTICATION METHOD FOR KEYLESS ENTRY SYSTEM

FIELD OF THE INVENTION

This invention relates to a keyless entry system for a motor vehicle or other protected environment, and particularly to a cryptographic method of secure communication for a keyless entry system.

BACKGROUND OF THE INVENTION

Personal-size remote control transmitters are widely used to provide a convenient method of locking or unlocking vehicles, and/or to remotely arm or disarm vehicle theft deterrent systems. They are also used to control home/business security systems and garage door openers. If these transmissions can be spoofed or played back, then these systems can be controlled by unauthorized parties to gain unwanted access to the protected environment. Most, if not all, of these systems provide very little protection against spoofing and no protection at all against the playback of legitimate messages that have been recorded and/or modified. The term "spoofing" as used herein refers to the creation of a false message that is accepted by the system as a valid message.

Conventional vehicle keyless entry systems prevent accidental interference from other transmitters through the use of frequency separation and identification codes. Some manufacturers use only one frequency, while others may have a number of frequencies available (but usually only one is used in any given system). Identification codes are then used to further ensure that one person's transmitter will not accidentally control someone else's system. These systems typically prevent guessing the identification code (usually between 16 and 32 bits) with penalty functions that limit the rate at which transmissions can be processed. For example, limiting receptions to one per second places a limit on how long it might take a thief to find the correct identification number by trying all possible combinations. However, these systems will accept any previously transmitted message that had been recorded and played back at any time in the future. Playback attacks can therefore be implemented very inexpensively, and such attacks are known to be used by professional car thieves who target specific vehicles. Since a successful attack will usually unlock the doors and simultaneously disarm alarm and ignition disable systems, the risk of being caught is significantly reduced.

A simple method of preventing playback attack is to include a simple dynamic security code in the message that changes with each transmission. The receiver calculates the next code in the sequence, and accepts a message as valid only if the received code matches the expected code. This method is insecure for three reasons. First, a thief can predict the next code sequence from knowledge of previous sequences, in much the same way as the receiver can predict which sequence to expect based on the last transmission. Second, once the code sequence has been determined, it can be used to issue false commands to all similar receivers. Third, the algorithm used to generate the code sequence must usually be kept secret, because a thief can much more easily predict the code sequences when the algorithm is known.

Message authentication using cryptographic techniques is a better method for preventing spoofing and playback attacks. However, applying conventional message authentication to personal transmitter-based systems has not been

used in the past since the available authentication algorithms have been too complex for implementation in very low cost systems. In addition, significantly larger message sizes were necessary to accommodate cryptographic synchronization, and the resulting increase in transmission time significantly reduced the expected life of the miniature batteries typically used.

SUMMARY OF THE INVENTION

It is therefore an object of the invention to generate very secure authenticated messages requiring a short transmission time to economize battery life in a personal transmitter. Another object is to obtain an exceptionally high level of protection from spoofing and playback attacks from a relatively short authenticated message. Still another object is to maintain a high level of security even where details of the security mechanisms and their implementation are known to an adversary.

The invention as described herein is not vulnerable to these types of attacks, multiple frequencies are not necessary, very inexpensive single-chip microcontrollers can implement all of the functions and quickly execute them, battery life is extended due to a unique message protocol that minimizes the amount of information that must be transmitted while maintaining a high level of security, and field support is simplified since transmitters and/or receivers can be easily replaced by authorized dealerships without the need for ordering a customized replacement from the factory.

A vehicle keyless entry system is composed of a transmitter for use by the vehicle's driver, and a receiver located within the vehicle. The transmitter emits RF signals in response to the activation of one or more buttons. The receiver periodically checks for the presence of a transmission, and performs the requested function only if fields within the message are intended for that particular receiver and it contains a valid security code.

A cryptographically based dynamic security code is included in the message structure to prevent the recording and subsequent playback of legitimate messages, and to prevent a receiver from being deceived into accepting messages from unauthorized sources. The security code sequence is determined by cryptographic techniques to assure that it is not predictable from knowledge of past sequences.

Once a transmitter is manufactured, it is programmed with a transmitter identification (ID), a default sequence number, a randomly generated initial seed, and a cryptographic key. The transmitter ID and initial seed are unique to each transmitter. The cryptographic key may be common to all transmitters, common only to some number of transmitters, or unique to each transmitter. The randomly generated initial seed is used as the starting point from which the authentication algorithm advances with each transmission. The sequence number also advances with each transmission to indicate to the receiver the required number of advances that it must perform to cryptographically synchronize with the transmission.

Future code sequences cannot be predicted from past sequences because each sequence is dependent on information selected by the operator just prior to transmission (e.g., information identifying which button was actuated) as well as the mechanics of the algorithm itself. The algorithm also does not need to be kept secret; only the cryptographic key which defines its specific mathematical operations needs to

be kept secret. Since this key can be unique to each individual transmitter and can be easily programmed during system fabrication, knowledge of the algorithm does not reduce the level of security provided by the system. In addition, because each transmitter/receiver pair generates a completely different sequence of codes, knowledge of one such sequence cannot be used to issue false commands to other receivers.

Receivers must be programmed to accept messages from one or more particular transmitters. In the preferred embodiment, the transmitter sends a special message which contains the transmitter ID, initial seed and cryptographic key. The receiver records this information in non-volatile memory so that it may recognize that transmitter in the future. An alternate method is to program this information directly into the receiver during its fabrication, but the preferred method should be retained to easily re-program a receiver to accept new transmitters in the field in case a transmitter is lost or the receiver becomes damaged or fails. A program switch is provided within the vehicle to enable this receiver function and to prevent transmissions from unauthorized transmitters from altering this information.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other advantages of the invention will become more apparent from the following description taken in conjunction with the accompanying drawings wherein like references refer to like parts and wherein:

FIG. 1 is a block diagram illustrating a keyless entry system for a motor vehicle;

FIG. 2 is a block diagram illustrating the keyless entry system with authenticated communication according to the invention;

FIG. 3 is an illustration of message structure for normal messages according to the invention;

FIG. 4 is an illustration of message structure for receiver programming according to the invention; and

FIG. 5 is a schematic diagram of a prior art cryptographic algorithm design which is useful in carrying out the invention.

DESCRIPTION OF THE INVENTION

Although the ensuing description is directed to a vehicle keyless entry system, it applies as well to garage door operators and to home or business security systems.

FIG. 1 shows a keyless entry system for a motor vehicle which includes a number of portable remote controls or fobs 10 small enough to carry in one's pocket or on a key chain. Each fob 10 has buttons 12 for manual selection of desired functions to be performed in the vehicle, a microprocessor 14 responsive to button actuation for formulating a command message, including an authenticator code and a function code identifying the desired function to be performed, and a radio transmitter 16 for transmitting the message. The fob 10 functions are supported by a miniature battery, not shown, which should have a life of several years. In the vehicle a receiver 18 receives the transmitted message, if the vehicle is within the transmitter range, and a microprocessor 20 acts upon data in the received message to determine whether the authenticator code is valid, and if so, to perform the desired function.

Each microprocessor 14 and 20 is programmed to execute a cryptographic algorithm which operates on certain stored and/or transmitted data, as well as on a selected function

code to generate an authentication code which is different for every transmission, thus preventing successful replay of a previously transmitted message. The authentication code is sufficiently short to be transmitted economically but the generation procedure has a complexity that renders it impractical for an adversary to predict the next valid code based on knowledge of previously transmitted messages. The procedure for message validation is first to compare the transmitter ID with IDs stored in the receiver memory, and if an ID match is found, then for the algorithm in the microprocessor to operate on a combination of shared secret data and transmitted data to produce authentication codes, and to determine that the command is valid if the codes are the same.

Two mechanisms are jointly used to assure that the authentication code changes in an unpredictable manner. First, the algorithm operates on a seed code which is changed according to a set of rules for each transmission. A sequence number is also incremented with each transmission and is included in the message so that the receiver algorithm will know how many seed code changes to execute in order to resynchronize with the transmitter since the receiver does not necessarily receive each transmission. Second, the authenticator code is generated as a function of the seed code and the cryptographic key as well as the desired function code. Since for each transmission the function code depends on which button the operator selects, another level of complexity is added to the authenticator code generation to confound attempts to determine a predictable progression of codes.

The upper portion of FIG. 2 illustrates the data inputs to the transmitter algorithm and to various fields of the transmitted message, and the authenticator code which is the product of the algorithm and also forms a field of the message. A cyclic redundancy code (CRC) is also calculated from all the other field data and included in the message. The unique ID assigned to each transmitter also forms a field of each message, but the ID does not enter the algorithm calculation. The algorithm may be any cryptographic-based authentication algorithm. Typically the specific procedures of such an algorithm will be determined by the mathematical function, a key, and on an initial working state known as a seed. Here the seed value is initially programmed into the transmitter, but the seed value is then updated with each transmission and is stored separately. This continuously updated seed value is used as the initial state of the algorithm for the calculation of each authenticator. The initial seed, the key, and the ID are permanently stored in each transmitter. A sequence number, beginning at 1, is incremented with each transmission. A function code representing a command to lock doors, unlock doors, etc. as selected by the buttons from a table of stored function codes, is also input to the algorithm which then generates an authenticator code as a function of the current seed and the function code. The message to be transmitted is then assembled and includes a preamble, the selected function code, the transmitter ID, the sequence number, the authenticator, and the CRC, as shown in FIG. 3.

The lower part of FIG. 2 represents the receiver functions which includes a memory for each associated transmitter comprising its ID, its key, its last calculated seed value, its last reported sequence number, and its initial seed value. When a message is received the CRC is verified, the transmitted ID is matched to one of the stored IDs and the stored data related to that ID is used by the algorithm along with the transmitted function code and sequence number to generate a receiver authenticator. If it is equal to the trans-

mitted authenticator message is verified as legitimate and the operation indicated by the function code is performed. In case the stored sequence number is less than the one in the message, the algorithm will advance the seed value and the sequence number until the sequence numbers are equal; then the transmitter and receiver seed values will also be equal and the authenticator can be calculated.

Message Structure

The message structure for normal messages (e.g., door lock, door unlock, trunk/hatch release, and panic) is shown in FIG. 3. The preamble indicates the start of a message. The remaining fields compose the actual command. The function code identifies the operation being requested, and corresponds to one or more switch actuations. The transmitter ID is a unique binary value associated with each individual transmitter. The sequence number is used to synchronize the transmitter and receiver to account for situations in which messages are received in error due to RF noise, or the transmitter is operated beyond the range of the receiver, or when the transmitter battery is replaced. The receiver will only perform the requested operation when a transmitter ID is recognized as belonging to that receiver, and the authenticator is verified.

Message playback is prevented since the sequence number is incremented with each transmission, therefore recorded messages (i.e., those with smaller than expected sequence numbers) will not be accepted. Spoofing of messages is prevented since modifying the function code (from a lock command into an unlock command, for example) will cause the receiver to calculate an incorrect authenticator. Since the authentication algorithm uses a cryptographic key known only to the transmitter and receiver, unauthorized parties cannot generate the authenticator that corresponds to a function code of their choosing and therefore cannot construct messages that would be acted upon by the receiver. Authenticating the transmitter ID and sequence number is not required since the receiver will ignore messages with unexpected IDs, and an incorrect or modified sequence number will cause the authentication to fail since the authentication algorithm will not be in the correct state.

The message structure for a resynchronization message is identical to FIG. 3, except that the Sequence Number field contains a randomly generated value instead of the actual sequence number. The message structure for the receiver programming message is shown in FIG. 4.

Algorithm Example

A number of authentication algorithms are available in the literature and can be used within this invention. However, a linear feedback shift register (LFSR) with a non-linear output function will be used in the following descriptions due to its simplicity and effectiveness.

A schematic diagram of such an algorithm is shown in FIG. 5. The Working Register is a Galois form of a LFSR, and its feedback polynomial is determined by the contents of the Key Register. Keys should therefore represent primitive irreducible polynomials of a degree appropriate for the length of the Working Register for maximum cryptographic strength, but randomly selected binary sequences can also be used. The ROM implements a table containing non-linear binary sequences that translates an n-bit linear input (n is 6 in this example) to a single non-linear binary output. A series of such outputs are concatenated to create the actual authenticator.

In practice it is preferred to implement the algorithm in software executed by a microprocessor. Due to the unique message structure and the dynamic involvement of the function code field in the algorithm process, a small in-

pensive microprocessor is capable of achieving a high level of security in the authenticator and at the same time limiting the authenticator to a short length to minimize transmission time and to thereby economize on battery life.

Transmitter Operation

The following description illustrates the typical operations performed when a transmitter button is pressed. It is assumed that a key and an initial seed have been programmed into the transmitter and receiver.

```

BEGIN normal message transmission
  Determine the function code (FC)
  Load the Working Register (WR) with the previous seed
  Increment the WR x times with input data = "V"
  Save the WR state
  Increment and save the sequence number (SN)
  Mod-2 add the FC to the WR feedback bit-by-bit and
  increment the WR
  Increment the WR y times
  Increment the WR z times and read the authenticator output
  Assemble the message, calculate the CRC, and transmit
  the message
END normal message transmission.
  
```

When a transmitter button is pressed, its corresponding function code is determined. The previous state of the Working Register is then read from memory and loaded into the Working Register. (For the first operation, it is the initial seed.) The Working Register is then incremented x times, with the input data being x "0"s. The resulting state of the Working Register is then saved back to memory, replacing the previously saved seed, and the sequence number is incremented. The function code is then modulo-2 added to the Working Register feedback on a bit-by-bit basis. The Working Register is then incremented y times. The Working Register is then incremented an additional z times, with the z bits generated by the algorithm saved for transmission as the authenticator. (The values of x and y are dependent on the particular authentication algorithm used, and z is determined by the desired length of the authenticator. Typical values for the algorithm previously defined are x=8, y=32, and z=24 to provide a high level of security while conserving battery power. Other values could be used, however.)

Receiver Operation

The following description illustrates the typical operations performed when a message is received:

```

BEGIN normal message reception
  If the message CRC is verified then continue else done
  If the transmitter ID is recognized then continue else done
  If the received SN is no more than k increments
  greater than the last SN then continue else done
  Load the WR with the previous seed corresponding to
  that transmitter ID
  Repeat
    Increment the WR x times with input data = "0"
    Increment the sequence number corresponding to that
    transmitter ID until the sequence number is equal to the
    received SN
  Save the WR state in temporary storage
  Mod-2 add the received FC to the WR feedback bit-by-
  bit and increment the WR
  Increment the WR y times
  Increment the WR z times and read the authenticator output
  If the calculated authenticator is equal to the
  received authenticator then continue else done
  Save the WR state held in temporary storage for that
  transmitter ID for use as the next seed
  Save the SN for that transmitter ID
  Act on the received function code
END normal message reception.
  
```

Upon receipt of an error-free message with a recognized transmitter ID, the receiver will compare the received

sequence number with the sequence number of the last valid message. If the sequence number is equal to or less than the previous one or ahead by more than k increments, the message will be ignored. (Typical values of k may range from 64 to 512.) If the received sequence number is greater by not more than k increments, the receiver will load the Working Register with the seed that corresponds to that particular transmitter ID. (This allows the receiver to automatically resynchronize to the transmitter to recover from those situations in which messages are received in error due to RF noise, or the transmitter is operated beyond the range of the receiver. It also allows one receiver to operate with multiple transmitters.) The receiver will increment the algorithm x times with the input data being "0"s, and increment its sequence number once. This process is repeated until the receiver's sequence number equals the received sequence number. The state of the Working Register is then temporarily saved for later use. The received function code is then modulo-2 added to the Working Register feedback on a bit-by-bit basis. The Working Register is then incremented y more times. The Working Register is incremented an additional z times, and the z bits generated by the algorithm are compared to the received authenticator. If the authenticators were not equal, the message will be ignored. If they were equal, the state of the Working Register temporarily saved earlier in the process will be saved for later use, replacing the previous seed. The new sequence number would then also be saved, and the receiver would perform the operation indicated by the received function code.

Resynchronization

Since this invention does not use two-way communication, another method was necessary to recover from situations in which the transmitter and receiver lose cryptographic synchronization. This method provides three different forms of resynchronization, depending on the extent of the synchronization loss.

The first level of resynchronization occurs when the transmitter's sequence number is greater than the receiver's by not more than k increments. In this case, the receiver will automatically advance to the transmitter's sequence number and then authenticate the message.

The next level of resynchronization allows recovery when the transmitter's sequence number is greater than the receiver's by more than k increments. This function must be initiated by the user, typically by depressing two buttons simultaneously. (This will usually only be required when the transmitter's battery is replaced.) The following special processing is performed:

```

BEGIN resync message transmission
  Determine the function code (FC)
  Generate a random number (R)
  Load the Working Register (WR) with the original initial
  seed
  Increment the WR (R+S) times with input data = "0"
  Save the WR state for use as the next seed
  Reset and save the sequence number (SN)
  Mod-2 add the FC to the WR feedback bit-by-bit and
  increment the WR
  Increment the WR  $y$  times
  Increment the WR  $z$  times and read the authenticator output
  Assemble the message with R in the Sequence Number
  field, calculate the CRC, and transmit the message
END resync message transmission.

```

Typical values of R and S may range from 32 to 256. The receiver will perform the following processing when this resynchronization message is received:

```

BEGIN resync message reception
  If the message CRC is verified then continue else done
  If the transmitter ID is recognized then continue else done
  Load the WR with the original initial seed
  corresponding to that transmitter ID
  Increment the WR (R+S) times with input data = "0"
  Save the WR state in temporary storage
  Mod-2 add the received FC to the WR feedback bit-by-
  bit and increment the WR
  Increment the WR  $y$  times
  Increment the WR  $z$  times and read the authenticator output
  If the calculated authenticator is equal to the
  received authenticator then continue else done
  Save the WR state held in temporary storage for that
  transmitter ID for use as the next seed
  Reset and save the SN for that transmitter ID
END resync message reception.

```

The final level of resynchronization (or initialization) is used to program the receiver to recognize the particular transmitter. This should only be required when transmitters or the receiver are replaced due to loss or failure. (It can also be used by the keyless entry system manufacturer to initially pair transmitters to a receiver.) Transmission of this message, shown in FIG. 4, must also be manually initiated, for example by depressing two buttons and holding them down for some length of time. In order for this message to be acted upon by the receiver, the receiver must be set in a program mode by a program switch 22 (FIG. 1). For example, a jumper is inserted into a special connector located somewhere within the vehicle. The following special processing is performed:

```

BEGIN receiver programming message transmission
  Determine the function code (FC)
  Assemble the message, calculate the CRC, and transmit the
  message
  Delay and transmit the message again
END receiver programming message transmission.

```

The receiver will perform the following processing when a receiver programming message is received:

```

BEGIN receiver programming message reception
  If the message CRC is verified then continue, else done
  If the program switch is activated, data continue else done
  Erase all information related to previously programmed
  transmitters
  Save the received transmitter ID, initial seed, and
  cryptographic key of the first transmitter
  Repeat for other transmitters until the program switch
  is reset
END receiver programming message reception.

```

Security Analysis

The ability of this invention to provide a high level of message protection depends on a number of factors. For example, the length of the authenticator and key space of the algorithm must be selected to minimize the likelihood that an exhaustive search can succeed. The algorithm must also be designed to avoid any mathematical weaknesses that would allow valid authenticators to be created, or its keys to be recovered, using analytical techniques alone. The system itself must also be considered, since improper implementation of the security mechanisms may introduce additional vulnerabilities that can be exploited by an adversary. In the limit, no attack scenario should be successful in less time or with fewer resources than required for an exhaustive search. The invention meets these requirements.

Playback and Spoof Attacks

This invention uses cryptographic authentication to protect keyless entry systems from accepting recorded messages that have been played back as well as those that have been modified and played back. It also protects against transmitters intended to deceive the receiver into accepting unauthorized messages as legitimate.

Recorded messages will not be accepted as valid due to the sequence number and authenticator. For example, the receiver's sequence number is incremented with each valid reception, and it will not accept messages with an equal or smaller sequence number. In addition, the sequence number itself cannot simply be modified since that would alter the authenticator calculated when the false message is received.

The message also cannot be modified in such a way as to be acceptable to the receiver since the authenticator is based on mathematically complex interactions among the algorithm, the key, a unique initial seed, and the function code. Even if the algorithm and key are known to a thief, he will not know the initial seed for any particular transmitter since they are unique to each transmitter and are generated randomly when the transmitters are programmed during their manufacture. Without knowledge of the initial seed, possession of the algorithm, key, and sequence number will not allow a valid authenticator to be economically generated for any given function code.

The same reasoning applies to messages from unauthorized transmitters intending to deceive a receiver into accepting function codes of the thief's choice. A valid authenticator cannot be calculated for any given transmitter without knowledge of its unique initial seed, even if the thief knows the algorithm, key, and sequence number.

A recorded message also cannot be played back to a different receiver since their initial seeds are different. This would cause the authenticators to fail, even if the transmitter ID and sequence numbers were modified to be valid for that receiver and the proper key was used.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. In a keyless entry system for performing any of a plurality of functions in a protected environment and having a receiver and at least one remote transmitter, the method of encoding a command for transmission to the receiver and for authenticating the command comprising the steps of:

installing into each transmitter and the receiver a cryptographic algorithm including a programmable cryptographic key for defining mathematical operations of the algorithm, a transmitter ID and an initial seed code peculiar to each transmitter, and a plurality of function codes;

in the transmitter:

selecting a function code for performing a predetermined function,

calculating an authenticator code by the algorithm as a function of both the seed code and the function code, and

transmitting the transmitter ID, the function code and the authenticator code to the receiver; and in the receiver:

verifying the transmitter ID by comparing with an ID installed in the receiver;

then calculating an authenticator code by the algorithm as a function of both the transmitted function code and the seed code; and

verifying the transmission by comparing the transmitted authenticator code with the receiver calculated authenticator code.

2. The invention as defined in claim 1 including the steps of:

in the transmitter, changing the seed code to a new value according to a predetermined function upon each transmission and replacing the seed code with the new value;

in the receiver, changing the seed code to a new value according to the same predetermined function for each transmission and replacing the seed code with the new value, whereby the seed code progressively changes in the same manner in both transmitter and receiver.

3. The invention as defined in claim 1 including the steps of:

installing a sequence number in the transmitter and receiver;

in the transmitter, updating the sequence number and the seed code to new values each according to a predetermined function upon each transmission and storing the updated values;

transmitting the current sequence number with each transmission;

in the receiver, synchronizing with the transmitter by updating the sequence number and the seed code according to the same predetermined functions until the receiver sequence number matches the transmitted current sequence number, thereby changing the seed code in the receiver to the same value as the transmitter seed code.

4. The invention as defined in claim 3 wherein each time the seed code is updated it is advanced through a predetermined plurality of states, so that sequential transmitted authenticator codes do not correspond to sequential algorithm states.

5. The invention as defined in claim 3 including the steps in the receiver of:

comparing the transmitter sequence number and the receiver sequence number;

determining the transmission to be invalid if the transmitted sequence number corresponds to a transmission prior to the current receiver sequence number.

6. The invention as defined in claim 3 wherein the step of updating the sequence number comprises incrementing the sequence number, and including the steps of:

comparing the transmitter sequence number and the receiver sequence number; and

terminating the receiver calculations if the transmitter sequence number is lower than the receiver sequence number.

7. The invention as defined in claim 1 wherein in the transmitter and the receiver the step of calculating the authenticator code comprises:

operating on the seed code and the function code by the algorithm to produce a sequence of data bits; and

converting the data bits to an authenticator code by a nonlinear conversion, whereby the transmitted authenticator code does not reveal the direct output of the algorithm.

8. In a keyless entry system for performing a predetermined function in a protected environment having a receiver and at least one remote transmitter, the method of encoding a command for transmission to the receiver and for authenticating the command comprising the steps of:

installing into each transmitter and the receiver a cryptographic algorithm including a key for defining the algorithm operation, a transmitter ID, a sequence number and an initial seed code peculiar to each transmitter, and a plurality of function codes;

11

in the transmitter:

selecting a function code for performing the predetermined function;

calculating an authenticator code by the algorithm as a function of both the seed code and the function code;

updating the seed code and the sequence number; and

transmitting the transmitter ID, the sequence number, the function code and the authenticator code to the receiver; and in the receiver:

verifying the transmitter ID by comparing with an ID installed in the receiver;

if the receiver sequence number corresponding to the verified ID is within a limited number of increments of the transmitted sequence number, updating the seed code corresponding to the transmitted ID and the receiver sequence number until the receiver sequence number matches the transmitted sequence number;

then calculating an authenticator code by the algorithm as a function of both the transmitted function code and the updated seed code; and

verifying the transmission by comparing the transmitted authenticator code with the receiver calculated authenticator code.

9. The invention as defined in claim 8 including the method of resynchronizing the transmitter and receiver when the receiver sequence number corresponding to the verified ID is not within the limited number of increments of the transmitted sequence number, comprising the steps of:

in the transmitter:

selecting a random number R;

updating the initial seed code a number of times equal to the product of R and s, where s is a predetermined number stored in both the transmitter and the receiver;

setting the sequence number to a default value;

generating an authenticator code by the algorithm using the updated seed code; and

transmitting the random number R and the authenticator code to the receiver; and in the receiver:

updating the initial seed code a number of times equal to the product of R and s;

generating a receiver authenticator code by the algorithm using the updated seed code; and

if the transmitted authenticator code and the receiver authenticator code are equal, then setting the sequence number to the default value and saving the updated seed code.

10. The invention as defined in claim 1 including the method of programming the receiver to recognize the transmitter wherein only the transmitter is programmed with a cryptographic key, a transmitter ID and the initial seed code, comprising the steps of:

manually enabling the receiver for initialization;

assembling a message in the transmitter including the ID, the key and the initial seed code;

calculating a cycle redundancy code CRC for the message;

transmitting the message and the CRC to the receiver; verifying the CRC in the receiver; and

then storing in the receiver the transmitter ID, the key and initial seed code related to that ID, whereby the transmitter and receiver are synchronized for authenticated communication.

11. The invention as defined in claim 1 wherein the step of installing into each transmitter and the receiver comprises the steps of:

installing the cryptographic algorithm and a plurality of function codes into each transmitter and the receiver upon manufacture;

12

programming the transmitter upon manufacture with a cryptographic key for defining the mathematical operations of the algorithm, a transmitter ID and the initial seed code;

manually enabling the receiver for initialization;

assembling a message in the transmitter including the transmitter ID, the key and the initial seed code;

calculating a CRC for the message;

transmitting the message and the CRC to the receiver; verifying the CRC in the receiver; and

then storing in the receiver the transmitter ID, the key and the initial seed code related to that ID, whereby the transmitter and receiver are synchronized for authenticated communication.

12. In a keyless entry system having a remote transmitter for commanding any of a plurality of functions in a protected environment and a receiver for responding to the commands and carrying out the commanded function, a secure communication method carried out by a cryptographic algorithm in both the transmitter and receiver for generating an authenticator code, wherein each algorithm includes a working register and means for incrementing the register with input data to produce an authenticator output and working register feedback; the communication method comprising the steps of:

incorporating into the transmitter and the receiver a cryptographic key for determining the mathematical operations of the algorithm, a transmitter ID, and an initial register state for the working register; a function code for each function, and integers y and z;

in the transmitter:

a) determining a function code for performing the commanded function;

b) loading the working register with the register state;

c) modulo-2 adding the function code to the working register feedback bit-by-bit and incrementing the working register for each function code bit;

d) incrementing the working register y times;

e) incrementing the working register z times and reading the authenticator output;

f) transmitting a message including the transmitter ID, the function code and the authenticator code; and in the receiver:

g) verifying the ID by comparing with an ID stored in the receiver;

h) executing steps a through e using the received function code, and the receiver register state to generate a receiver authenticator code;

and verifying the transmission by comparing the transmitted authenticator code with the receiver authenticator code.

13. The invention as defined in claim 12 wherein the transmitter and receiver are programmed with a sequence number and an integer x, and

in the transmitter, after step b, including the steps of:

i) incrementing the working register x times with input data equal to zero;

j) saving the register state;

k) incrementing and saving the sequence number; and

l) transmitting the sequence number as part of the message; and

in the receiver:

computing the receiver sequence number with the transmitted sequence number; and

repeating steps i through k until the receiver sequence number is equal to the transmitted sequence number.

* * * * *